

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of)
)
 Information associated with One (1) Target) Case No. MJ21-567
 Accounts/Identifiers, for Investigation of 21)
 U.S.C. §§ 841 & 846 and Other Offenses)

APPLICATION FOR A SEARCH WARRANT AND PEN-TRAP ORDER

I, a federal law enforcement officer or an attorney for the government, request a search warrant and pen-trap order, and state under penalty of perjury that I have reason to believe that on the person or property described in Attachment A2, located in the Western District of Washington, there is now concealed property and evidence described in Attachment B2. This Court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. §§ 841 & 846

Offense Description
 Distribution and Conspiracy to Distribute Controlled Substances

The application is based on the facts set forth in the attached affidavit, which is incorporated herein by reference with all attachments and exhibits. Pursuant to 18 U.S.C. § 3123(a)(1), Exhibit 1 to the affidavit includes a certification from an attorney from the government that the requested information is relevant to an ongoing criminal investigation.

Pursuant to Fed. R. Crim. P. 41, this warrant is presented by:

- ☒ by reliable electronic means; or ☐ telephonically recorded


Applicant's signature

Joseph Kirby, DEA TFO
Printed name and title

- ☐ The foregoing affidavit was sworn before me and signed in my presence, or
☒ The above-named officer provided a sworn statement attesting to the truth or the foregoing affidavit by telephone.

Date: October 22, 2021


Judge's signature

Paula McCandlis, United States Magistrate Judge
Printed name and title

City and state: Bellingham, Washington

ATTACHMENT A2**Property to Be Searched and Subscriber/Subject Information**

1. Records and information associated with the cellular phone assigned call number (360) 230-0625, ("Target Telephone 2" or the "Target Phone"), that are in the custody or control of T-Mobile, a company headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054. The subscriber/customer of the Target Cell Phone is "Mario GARCIA" with an address of "11400 NE 132nd Street Apt B106 Kirkland, Washington, 98034-4752.". The identity of the person who is the subject of the criminal investigation is unknown.

2. The property to be searched includes: (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number assigned to an instrument now bearing the same unique identifying number (such as an IMSI, ESN, MSID, or IMEI) as the telephone number listed above, or that was bearing the same unique identifying number as the telephone number listed above, at any point within the last 30 days, (iii) any changed unique identifying number subsequently assigned to the same telephone number, or (iv) any additional changed telephone number and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone numbers listed above, within the period of disclosure authorized by this warrant.

In Attachment B2, T-Mobile may be referred to as the "Wireless Provider."

ATTACHMENT B2

Particular Things to be Seized

This warrant is issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2713, and the Pen Register Act, 18 U.S.C. §§ 3121-3127. As such, this warrant authorizes the collection of subscriber records, pen-trap data, and cell site data information regarding the Target Cell Phone. **This warrant does not authorize the disclosure or seizure of any tangible property or the content of any wire or electronic communication, as defined in 18 U.S.C. § 2510(8).** Accordingly, the Court finds reasonable necessity for the seizure of the data and records identified below. *See* 18 U.S.C. § 3103a(b)(2).

I. Section I: Information to be Disclosed by T-Mobile

1. **Subscriber/Account Information.** The following non-content information about the customers or subscribers associated with the Account listed in Attachment A2:

- a. Names (including subscriber names, user names, and screen names);
- b. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- c. Local and long distance telephone connection records from September 21 to October 22, 2021;
- d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions from September 21, 2021 to October 22, 2021;
- e. Length of service (including start date) and types of service utilized;
- f. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital

1 Network Numbers (“MSISDN”), International Mobile Subscriber Identity Identifiers
 2 (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

3 g. Other subscriber numbers or identities (including the registration
 4 Internet Protocol (“IP”) address); and

5 h. Means and source of payment for such service (including any credit
 6 card or bank account number) and billing records.

7 **2. Pen Register/ Trap and Trace Data and Associated Subscriber Records**
 8 **to Be Provided for a Period from October 22, 2021 to December 6, 2021.**

9 a. The T-Mobile shall install and monitor pen-trap devices to record,
 10 decode, and/or capture dialing, routing, addressing, and signaling information associated
 11 with each communication to or from the Target Cell Phone including the date, time, and
 12 duration of the communication, and the following, without geographic limit and without
 13 notice to the subscriber:

14 (i) IP addresses associated with the cell phone device or devices used to send
 15 or receive electronic communications;

16 (ii) Any unique identifiers associated with the cell phone device or devices
 17 used to make and receive calls with the cell phone number described in
 18 Attachment A2, or to send or receive other electronic communications,
 19 including the ESN, MEIN, IMSI, IMEI, SIM, MSISDN, or MIN;

20 (iii) IP addresses of any websites or other servers to which the cell phone device
 21 or devices connected; and

22 (iv) Source and destination telephone numbers and email addresses.

23 b. On a 24-hour-a-day basis, for the duration of the authorized pen-trap
 24 devices, T-Mobile shall provide the following records for those subscribers whose
 25 identifiers are obtained pursuant to the use of the pen-trap devices: published or non-
 26 published subscriber names and addresses, including billing addresses.

1 **3. Historical Cell Site Location Information.**

2 a. All records and other information (**not including the contents of**
3 **communications**) relating to wire and electronic communications sent or received by the
4 Account from **September 21, 2021**, including:

5 i. the date and time of the communication, the method of the
6 communication, and the source and destination of the communication (such as the source
7 and destination telephone numbers (call detail records), email addresses, and IP
8 addresses); and

9 ii. historical cell site information regarding the cell tower and
10 antenna face (also known as “sectors”) through which the communications were sent and
11 received. This information is to be provided irrespective of the application, name, or
12 report utilized by the T-Mobile. Accordingly, this information includes the following
13 data sets to the extent that they are collected by the T-Mobile: RTT, PLU, PCMD,
14 NELOS, EVDO, TruCall, ALULTE, and Timing Advance.

15 b. The physical address and coverage maps of cell towers used by the
16 Target Cell Phone.

17 **4. Prospective Cell Site Location Information.**

18 a. All information about the location of the Target Cell Phone
19 described in Attachment A2 for from **October 22, 2021 to December 6, 2021**, during all
20 times of day and night. This information includes: precise location information, as well
21 as all data about which “cell towers” (i.e., antenna towers covering specific geographic
22 areas) and “sectors” (i.e., faces of the towers) received a radio signal from the cellular
23 telephone(s) or account(s) described in Attachment A2.

24 b. The physical address and coverage maps of cell towers used by the
25 Target Cell Phone.
26

27 To the extent that the cell site information described in the previous paragraphs
28 (hereinafter, “Location Information”) is within the possession, custody, or control of T-

1 Mobile, T-Mobile is required to disclose the Location Information to the government
2 pursuant to this warrant. In addition, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-
3 (b), T-Mobile must furnish the government all information, facilities, and technical
4 assistance necessary to accomplish the collection of the Location Information
5 unobtrusively and with a minimum of interference with T-Mobile's services. The
6 government shall compensate T-Mobile for reasonable expenses incurred in furnishing
7 such facilities or assistance.

8
9 **II. Section II: Information to Be Seized by the Government**

10 1. All information described above in Section I that constitutes evidence of
11 violations of 21 USC §§ 841 and 846 involving unidentified subjects.

12 2. All non-content subscriber/account information provided pursuant to 18
13 U.S.C. § 2703(c).

14 3. All non-content dialing, routing, addressing, and signaling information
15 provided pursuant to 18 U.S.C. §§ 3121-3127.

16 4. Location Information regarding the Target Cell Phone.
17 Law enforcement personnel (who may include, in addition to law enforcement
18 officers and agents, attorneys for the government, attorney support staff, agency
19 personnel assisting the government in this investigation, and outside technical experts
20 under government control) are authorized to review the records produced by the T-
21 Mobile in order to locate the things particularly described in this Warrant.

STATE OF WASHINGTON)
) SS
COUNTY OF WHATCOM)

I. INTRODUCTION

Application for a Tracking Warrant for One Target Telephone

a. **Target Telephone 2 (TT2)**, assigned call number (360) 230-0625, subscriber “Mario GARCIA” with an address of “11400 NE 132nd Street Apt 100, Washington, 98034-4752,” whose service provider is T-Mobile, a wireless service provider located at 4 Sylvan Way, Parsippany, New Jersey 07054. Service began for **TT2** on September 20, 2021. Investigators believe that **TT2** is used to facilitate drug trafficking activities.

3. The Court has jurisdiction to issue the proposed warrant under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2713, because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is the Western District of Washington, a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

//
//

Pen Register Act

4. Because this warrant seeks the prospective collection of information that falls within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to comply with the Pen Register Act, 18 U.S.C. §§ 3121-3127.

5. The Court has jurisdiction to issue the requested pen-trap order because it is a “court of competent jurisdiction” under 18 U.S.C. § 3122(a)(2). Specifically, the Court is a district court of the United States that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 3127(2)(A)(i).

6. This application includes all the information required by the Pen Register Act. *See* 18 U.S.C. §§ 3122(b) & 3123(a)(1). Namely, Exhibit 1 to this application is a certification from Assistant United States Attorney Stephen Hobbs that (1) identifies the Drug Enforcement Administration as the law enforcement agency conducting the investigation and (2) certifies the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. 18 U.S.C. § 3122(b). The Assistant United States Attorney is an “attorney for the government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

7. A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” 18 U.S.C. § 3127(4).

8. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications such as emails, text messages, connection logs, and data transfers. The

1 prospective location data sought in this application constitutes “dialing, routing,
2 addressing, and signaling information” covered by the Pen Register Act. Accordingly,
3 the requested warrant will record, decode, and/or capture dialing, routing, addressing, and
4 signaling information associated with the target cell phone without geographic limit.

5 9. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and
6 3124(a)-(b), that the Court order through Attachment B2 of the requested warrant that T-
7 Mobile and any other person or entity providing wire or electronic communication
8 service in the United States whose assistance may facilitate execution of this warrant
9 furnish, upon service of the warrant, information, facilities, and technical assistance
10 necessary to install the pen/trap, including installation and operation of the pen-trap
11 unobtrusively and with minimum disruption of normal service. Any entity providing
12 such assistance shall be reasonably compensated by the Drug Enforcement
13 Administration, pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in
14 providing facilities and assistance in furtherance of the warrant.

15 10. This is the first application in this judicial district for a search warrant
16 authorizing disclosure of the above information for **Target Telephone 2** in connection
17 with this investigation.

18 11. **Through this application, the United States does not request and does**
19 **not seek to obtain the contents of any communications, as defined in 18 U.S.C.**
20 **§ 2510(8).**

21 **Application for a Tracking Warrant for One Target Vehicle**

22 12. I am also submitting this Affidavit pursuant to Rule 41 of the Federal Rules
23 of Criminal Procedure in support of an application for a warrant authorizing the real-time
24 location tracking of **Target Vehicle 2** for a period of 45 days.

25 //

26 //

27 //

28 //

1 a. **Target Vehicle 2 (TV2)**, is a silver Jeep Grand Cherokee, bearing
 2 Washington license plate BZD4114 (hereinafter “**Target Vehicle 2**” or “**TV2**”).
 3 According to the Washington Department of Licensing **TV2** is registered to “Brian
 4 Fernando CASTRO CASTRO” at 2728 175th St SE Bothell, WA 98012. Investigators
 5 believe that **TV2** is being used to facilitate drug trafficking activities.

6 13. For the reasons described in greater detail below, I am seeking authority to
 7 enter the unfenced driveway and/or parking areas of the following location:

8 a. 7443 NE 146th Street Kenmore, WA 98028. This is the address that
 9 investigators followed **TV2** to, after the controlled purchase on September 29, 2021, as
 10 noted below.

11 b. 2728 175th St SE Bothell, WA 98012. This is the current registered
 12 address for **TV2** according to the Washington Department of Licensing.

13 14. We request permission to install/service the tracking device at any time,
 14 day or night, in order to ensure that we can do so covertly and avoid jeopardizing the
 15 ongoing investigation. Investigators believe it would be safer for investigators to install
 16 the tracking device(s) during hours of darkness, to ensure the tracking device is installed
 17 in a covert manner. The addresses listed above are visible from neighboring houses,
 18 which makes it highly unlikely that investigators will be able to install or maintenance the
 19 tracking device in a covert manner during daylight hours. Additionally, the addresses are
 20 difficult to access during daylight hours, as any foot traffic would be out of place, and
 21 could jeopardize the covert actions need to effectively and safely install the tracking
 22 device(s). Because we believe early morning hours or later evening hours are the safest
 23 time for installation and access to the vehicle, we request nighttime authorization.

24 15. I seek authority to do the following: (a) install, remove, monitor, repair, or
 25 adjust a global positioning satellite (hereinafter GPS) electronic tracking device on **TV2**
 26 at any time of the day or night; (b) if necessary to protect the safety of persons installing,
 27 removing, monitoring, repairing, or adjusting the electronic tracking device on **TV2**, or to
 28 protect the integrity of the investigation, to surreptitiously enter the subject vehicle at any
 time of the day or night, and move the subject vehicle from one location to another for
 the purpose of installing, removing, monitoring, repairing, or adjusting the device; and/or

1 to tow the vehicle; (c) surreptitiously re-enter **TV2** at any time of the day or night, for the
 2 purpose of installing, removing, monitoring, repairing, or adjusting the device; and
 3 (d) continuously monitor any and all signals emitted from the electronic tracking device
 4 in any jurisdiction within the United States, including when the vehicle enters any
 5 structure or private property in which there may be a reasonable expectation of privacy. I
 6 request this authorization for a period of up to forty-five (45) days.

7 16. I make this request based on the evidence described below, which
 8 establishes probable cause to believe that **TV2** is involved in criminal activity,
 9 specifically drug trafficking in violation of 21 U.S.C. §§ 841 and 846, and that the
 10 information collected pursuant to the warrant will include evidence of violations of 21
 11 U.S.C. §§ 841 and 846.

12 17. This is the first application in this judicial district for a tracking warrant for
 13 **TV2** in connection with this investigation.

14 **Application for a Facebook Search Warrant**

15 18. I also make this affidavit in support of an application for a search warrant
 16 for information associated with a certain Facebook user ID that is stored at premises
 17 owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social
 18 networking company headquartered in Menlo Park, California. The information to be
 19 searched is described in the following paragraphs and in Attachment A3. This affidavit is
 20 made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a),
 21 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government
 22 records and other information in its possession, pertaining to the subscriber or customer
 23 associated with the following user ID:

24 //

25 //

26 //

27 //

28 //

19. For the reasons stated in more detail below, I believe that the following offenses have been committed and are being committed by Julio CORRALES OCHOA (hereinafter, “CORRALES OCHOA”), and others:

a. Distribution of, and possession with intent to distribute, controlled substances (including but not limited to fentanyl), in violation of 21 U.S.C. § 841(a)(1);

b. Conspiracy to commit the foregoing offenses, in violation of 21 U.S.C. §§ 841 and 846;

20. I believe there is also probable cause to search the information described in Attachment A3 and Section I of Attachment B3 for evidence, instrumentalities, contraband or fruits of these crimes, as described in Section II of Attachment B3.

AGENT BACKGROUND

21. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7). Specifically, I am a Border Patrol Agent employed by the United States Border Patrol, Blaine Washington Sector. I have been employed as a Border Patrol Agent since August 2005. I am currently assigned as a Task Force Agent with the Drug Enforcement Administration (“DEA”), Bellingham, Washington Resident Office. I have worked as a Task Force Agent with the DEA since November 2015. In that capacity, I investigate violations of the Controlled Substances Act (Title 21, United States Code, Section 801, et seq.). In my experience as a law enforcement officer, I have participated in numerous narcotics investigations, during the course of which I have participated in physical surveillance, undercover operations, and executions of search warrants. I have arrested subjects attempting to smuggle narcotics, people, and other forms of contraband both into and out of the United States. I have participated in the debriefing of defendants, witnesses, and informants, during which time I have discussed with them their methods of drug smuggling, distribution, packaging, trafficking, avoiding law enforcement, among other

1 concerns related to drug trafficking. I have discussed and learned from other law
2 enforcement investigators in regard to these matters as well.

3 22. The facts in this affidavit come from my personal observations, my training
4 and experience, and information obtained from other agents and witnesses. This affidavit
5 is intended to show merely that there is sufficient probable cause for the requested
6 warrants and a pen-trap, and therefore does not set forth all of my knowledge about this
7 matter.

8 23. Based on the facts set forth in this affidavit, there is probable cause to
9 believe that violations of Title 21, United States Code, Sections 841 and 846, have been
10 committed, are being committed, and will be committed by the user(s) of **TA1, TT2**, and
11 a user/driver of 2 **TV2**, and that the **Target Account, Target Telephone and Target**
12 **Vehicle** described herein have been used in furtherance of those offenses. There is also
13 probable cause to believe that the location information described in Attachment B2, and
14 information described in attachment B3, will constitute evidence of these criminal
15 violations and will lead to the identification of individuals who are engaged in the
16 commission of these offenses as well as locations and other assets (such as vehicles and
17 real estate) that are used in the commission of these offenses.

18 SUMMARY OF PROBABLE CAUSE

19 A. The Investigation

20 24. The United States, including the Drug Enforcement Administration,
21 Homeland Security Investigations (hereinafter referred to as HSI) and Skagit County
22 Interlocal Drug Enforcement Unit (hereinafter referred to as SCIDEU) is conducting a
23 criminal investigation of Julio CORRALEZ OCHOA and others, regarding possible
24 violations of 21 U.S.C. 841(a)(1) (distribution of controlled substances) and 846
25 (conspiracy to distribute controlled substances).

26 1. Controlled Purchase Julio CORRALES OCHOA in September 2021

27 25. In September 2021, at the direction of law enforcement two SCIDEU
28 confidential sources (hereinafter "CS2" and "CS3") arranged for the purchase of drugs

1 from Julio CORRALES OCHOA. These arrangements were made between CS2 and
2 CORRALES OCHOA via Facebook Messenger. Investigators identified CORRALES
3 OCHOA'S Facebook Account as ID: 100001513642714 (**Target Account 1** or **TA1**).
4 Investigators examined Facebook messages between CS2 and CORRALES OCHOA and
5 learned that CS2 had been communicating with CORRALES OCHOA on **TA1** since
6 2017. Investigators also observed communications between CS2 and CORRALES
7 OCHOA (**TA1**) regarding the purchase of controlled substances; the drug
8 communications started in 2020.

9 26. CS2 and CS3 are cooperating for judicial consideration. CS2 has prior
10 felony convictions for identity theft and controlled substance possession. CS3 has prior
11 felony convictions for robbery, unlawful possession of a firearm, manufacturing/delivery
12 controlled substances, criminal impersonation, and bail jumping.

13 27. On September 29, 2021, investigators met with CS2 and CS3. At the
14 direction of law enforcement, CS2 arranged to purchase 500 counterfeit "M-30" pills,
15 suspected to contain fentanyl, for \$1,500 from the person who CS2 knows as Julio
16 CORRALES OCHOA. To set up the controlled purchase, CS2 used Facebook messenger
17 to contact CORRALES OCHOA on **TA1**. In the response, CORRALES OCHOA
18 instructed CS2 to drive to Tulalip, Washington, to meet with a drug courier or "runner" to
19 purchase the pills.

20 28. Prior to traveling to Tulalip, CS2 and CS3 met with investigators where
21 both CS2 and CS3, and their vehicle, were searched for significant amounts of US
22 currency, weapons, and other contraband; none was found. CS2 was subsequently
23 provided with \$1,500 in pre-recorded buy funds.

24 29. Investigators followed CS2 and CS3 to the arranged meeting location. CS2
25 and CS3 did not meet with anyone prior to their arrival at the meeting location. Shortly
26 after their arrival at the arranged meeting location, CS2 received a phone call (not
27 recorded) from a person who CS2 later identified as CORRALES OCHOA'S drug
28 courier, utilizing phone number (360) 230-0625 (**Target Telephone 2** or **TT2**). CS2 said

1 that during the call, the drug courier indicated he was en route to CS2 and CS3's
2 location.¹

3 30. A short time after this conversation investigators saw CS2 exit CS2's
4 vehicle get into a silver Jeep Grand Cherokee bearing Washington license plate BZD4114
5 (**Target Vehicle 2** or **TV2**). According to the Washington Department of Licensing,
6 BZD4114 is a 2011 Jeep Cherokee registered to "Brian Fernando CASTRO CASTRO" at
7 2728 175th Street SE Bothell, Washington, 98012. Law enforcement maintained
8 surveillance of **TV2** for a short amount of time before investigators saw CS2 get out of
9 the **TV2**, walk back to CS2's vehicle, and depart the area.

10 31. Investigators followed CS2 and CS3 from the meeting location and again
11 met with CS2 and CS3. CS2 and CS3 did not meet with anyone between leaving **TV2**
12 and the subsequent meeting with law enforcement. CS2, CS3, and their vehicle, were
13 again searched by investigators for weapons, large quantities of U.S. currency, and other
14 contraband; none was found. Investigators recovered the approximately 500 counterfeit
15 pills suspected to contain fentanyl from CS2. CS2 told investigators that CS2 met with
16 an unknown male in **TV2** who provided CS2 with the pills. CS2 paid the unknown male
17 for the pills with the \$1,500 pre-recorded buy funds. CS2 told investigators that, prior to
18 CS2's cooperation with law enforcement, CS2 has previously purchased drugs from this
19 same drug courier during previous deals with CORRALES OCHOA.

20 32. Following the meeting with CS2, investigators observed a Hispanic male,
21 and sole occupant of **TV2**, exit **TV2** and walk into a nearby shopping center.
22 Investigators noted that the Hispanic male closely resembled the driver's license
23 photograph of **TV2**'s registered owner, Brian Fernando CASTRO CASTRO.
24 Investigators maintained surveillance of **TV2** and observed the same Hispanic male
25 return to **TV2** a short time later and depart the parking lot. Investigators followed **TV2** to
26 Bothell, Washington where surveillance of the vehicle was lost for approximately twenty

27 ¹ CS2 was in contact with the handling investigator and providing updates during this time.
28

1 minutes. Investigators were able relocate **TV2** and observed the vehicle parked at a
2 residence located at 7443 NE 146th Street Kenmore, Washington, 98028. Investigators
3 observed **TV2** backed into the driveway of this residence and saw that **TV2** appeared to
4 be unoccupied. Surveillance was then terminated.

5 33. In sum, law enforcement believes that **TA1** and **TT2** were used at various
6 stages to arrange the controlled purchase of fentanyl pills, and that **TV2** was used to
7 transport those pills.

8 **KNOWLEDGE BASED ON TRAINING AND EXPERIENCE**

9 34. Based on my training, experience, and conversations with other
10 experienced narcotics investigators, I have gained experience in the techniques and
11 methods used by drug traffickers to distribute controlled substances, to include their use
12 of cellular phones and other electronic communication devices to facilitate their
13 trafficking activity. I know drug traffickers use cellular phones to communicate with
14 suppliers, re-distributors, and customers. These communications via cellular phone often
15 include discussing details around drug deals such as time and place of drug transactions,
16 types of drugs, amounts of drugs, methods of payment for drugs, and quality of drugs
17 sold or bought, amongst other things. I know that it is common for drug traffickers to use
18 multiple phones as well as change phone numbers regularly. They use different
19 telephones to help compartmentalize their drug trafficking activities. This might entail
20 using specific phones for their personal life and other phones for drug activity. Or it
21 might include using different phones for different individuals or aspects of their business,
22 such as using certain phones to contact suppliers and other phones to contact
23 redistributors. This compartmentalizing is especially common for individuals in
24 leadership positions. Drug traffickers often try to keep the various components and
25 organization members separate to protect parts of the organization from detection by law
26 enforcement. For example, if one individual or arm of a drug trafficking organization
27 (DTO) is arrested or seeks to assist law enforcement, that person could do less damage to
28 the organization if the leadership limits what he or she knows about other parts of the

1 DTO. Drug traffickers also use multiple cell phones to frustrate law enforcement
2 interception and monitoring. Where there are multiple cell phones, law enforcement may
3 learn of one part of the organization's activities by intercepting one phone, but they
4 would not receive information as to the overall activities of the DTO. Thus, the use of
5 multiple cell phones helps the survival of the overall organization.

6 35. Based on my training and experience, I know each cellular device has one
7 or more unique identifiers embedded inside it. Depending on the cellular network and
8 the device, the embedded unique identifiers for a cellular device could take several
9 different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic
10 Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber
11 Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network
12 Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an
13 International Mobile Equipment Identity ("IMEI"). The unique identifiers -- as
14 transmitted from a cellular device to a cellular antenna or tower -- can be recorded by
15 pen-traps and indicate the identity of the cellular device making the communication
16 without revealing the communication's content.

17 36. Based on my training and experience, I know that when a cell phone
18 connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the
19 cellular antenna or tower, and the cellular antenna or tower records those identifiers as a
20 matter of course. The unique identifiers -- as transmitted from a cell phone to a cellular
21 antenna or tower -- are like the telephone number of an incoming call. They can be
22 recorded by pen-trap devices and indicate the identity of the cell phone device making the
23 communication without revealing the communication's content. In addition, a list of
24 incoming and outgoing telephone numbers is generated when a cell phone is used to
25 make or receive calls, or to send or receive text messages (which may include
26 photographs, videos, and other data). These telephone numbers can be recorded by pen-
27 trap devices and then used to identify the parties to a communication without revealing
28 the communication's contents.

1 37. Based my training and experience, I know that a cell phone can also be
2 used to exchange text messages with email accounts. The email addresses associated
3 with those text messages can be recorded by pen-trap devices and then used to identify
4 parties to a communication without revealing the communication's contents.

5 38. Based on my training and experience, I know that cellular phones can
6 connect to the internet via a cellular network. When connecting through a cellular
7 network, internet communications sent and received by the cellular phone each contain
8 the same unique identifier that identifies cellular voice communications, such as an ESN,
9 MEIN, MIN, SIM, IMSI, MSISDN, or IMEI. Internet communications from a cellular
10 phone also contain the IP address associated with that cellular phone at the time of the
11 communication. Each of these unique identifiers can be used to identify parties to a
12 communication without revealing the communication's contents.

13 39. In my training and experience, I have learned that T-Mobile is a company
14 that provides cellular telephone access to the general public. I also know that certain
15 providers of cellular telephone service have technical capabilities that allow them to
16 collect and generate information about the locations of the cellular telephones to which
17 they provide service, including E-911 Phase II data (also known as GPS data or latitude-
18 longitude data) and cell-site data (also known as "tower/face information" or cell
19 tower/sector records). E-911 Phase II data provides relatively precise location
20 information about the cellular telephone itself, either via GPS tracking technology built
21 into the phone or by triangulating on the device's signal using data from several of the
22 provider's cell towers. Cell-site data identifies the cell towers (i.e., antenna towers
23 covering specific geographic areas) that received a radio signal from the cellular
24 telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the
25 telephone connected. These towers are often a half-mile or more apart, even in urban
26 areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to
27 a wireless device does not necessarily serve every call made to or from that device.
28 Accordingly, cell-site data is typically less precise than E-911 Phase II data.

1 40. Based on my training and experience, I know that T-Mobile can collect E-
2 911 Phase II data about the location of the Target Cell Phone, including by initiating a
3 signal to determine the location of the Target Cell Phone on T-Mobile's network or with
4 such other reference points as may be reasonably available.

5 41. When using a cellular connection to receive or transmit data, a cellular
6 phone typically utilizes a cell tower to make telephone calls, send or receive text
7 messages, send or receive emails, surf the internet, carry out application initiated data
8 transfers, among other things.

9 42. Based on my training and experience, I know that T-Mobile can collect
10 cell-site data about the Target Cell Phone. Based on my training and experience, I know
11 that for each communication (including data connections) a cellular device makes, its
12 wireless service provider can typically determine: (1) the date and time of the
13 communication; (2) the telephone numbers involved, if any; (3) the cell tower to which
14 the customer connected at the beginning of the communication; (4) the cell tower to
15 which the customer connected at the end of the communication; and (5) the duration of
16 the communication. I also know that wireless providers such as T-Mobile typically
17 collect and retain cell-site data pertaining to cellular devices to which they provide
18 service in their normal course of business in order to use this information for various
19 business-related purposes.

20 43. Different service providers use different systems, applications, and reports
21 to collect or analyze cell site data. These systems, applications, and reports are referred
22 to by a variety of names including, but not limited to real-time tool or "RTT" (Verizon),
23 Periodic Location Updates or "PLU" (Verizon), per call measurement data or "PCMD"
24 (Sprint), Network Event Location System or "NELOS" (AT&T), EVDO, ALULTE,
25 Timing Advance, and TruCall. RTT data, for example, estimates the approximate
26 distance of the cellular device from a cellular tower based upon the speed with which
27 signals travel between the device and the tower. This information can be used to estimate
28 an approximate location range that is more precise than typical cell-site data.

1 44. Based on my training and experience, I know that wireless providers such
2 as T-Mobile and Verizon typically collect and retain information about their subscribers
3 in their normal course of business. This information can include basic personal
4 information about the subscriber, such as name and address, and the method(s) of
5 payment (such as credit card account number) provided by the subscriber to pay for
6 wireless communication service. I also know that wireless providers such as T-Mobile
7 and Verizon typically collect and retain information about their subscribers' use of the
8 wireless service, such as records about calls or other communications sent or received by
9 a particular device and other transactional records, in their normal course of business. In
10 my training and experience, this information may constitute evidence of the crimes under
11 investigation because the information can be used to identify the Target Cell Phone's user
12 or users and may assist in the identification of co-conspirators and/or victims.

13 45. Modern cell phones allow users to switch their telephone numbers, use
14 multiple telephone numbers on a single device, and transfer their telephone number to a
15 different cell phone. These changes can be made with the assistance of the wireless
16 provider or by taking actions such as changing the "SIM card" (short for "subscriber
17 identity module card") of a cellphone. To provide for any such changes made to the
18 Target Cell Phone, Attachment A specifies that the property to be searched includes:
19 (i) any instrument to which the listed target telephone number was assigned within the
20 last 30 days, and that now has been assigned a changed telephone number, (ii) any
21 changed telephone number assigned to an instrument now bearing the same unique
22 identifying number (such as an IMSI, ESN, MSID, or IMEI) as the telephone number
23 listed above, or that was bearing the same unique identifying number as the telephone
24 number listed above, at any point within the last 30 days, (iii) any changed unique
25 identifying number subsequently assigned to the same telephone number, or (iv) any
26 additional changed telephone number and/or unique identifying number, whether the
27 changes occur consecutively or simultaneously, listed to the same subscriber and wireless
28

1 telephone account number as the telephone number listed above, within the period of
2 disclosure authorized by this warrant.

3 **AUTHORIZATION REQUEST FOR TARGET TELEPHONE 2**

4 46. Based on the fact set forth in this affidavit, there is probable cause to
5 conclude that violations of 21 U.S.C §841 and §846 (distribution of controlled substances
6 and conspiracy to distribute controlled substances) have been committed, are being
7 committed, and will be committed by Julio CORRALES OCHOA, and others who are
8 known and unknown. The requested information, including prospective location
9 information, for **Target Telephone 2** will help law enforcement monitor the user of the
10 Target Telephone, follow the movements when it is at locations that are otherwise hard
11 for law enforcement to observe, and identify other coconspirators, sources of supply,
12 storage locations, and other people and places of evidentiary value. There is probable
13 cause to believe that the use of the investigative technique described by the warrant will
14 result in officers learning that identifying information.

15 47. Based on the foregoing, I request that the Court issue the proposed search
16 warrant and pen-trap order for the Target Telephone, i.e., **Target Telephone 2** pursuant
17 to Federal Rule of Criminal Procedure 41, 18 U.S.C. § 2703(c), and 18 U.S.C. § 3123.

18 48. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of
19 Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to
20 delay notice to the subscriber or user of the Target Cell Phone until 90 days after the
21 collection authorized by the warrant has been completed. There is reasonable cause to
22 believe that providing immediate notification of the warrant may have an adverse result,
23 as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of
24 the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a
25 disclosure would give that person an opportunity to destroy evidence, change patterns of
26 behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1).
27 As further specified in Attachment B2, which is incorporated into the warrant, the
28 proposed search warrant does not authorize the seizure of any tangible property. *See* 18

1 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of
 2 any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire
 3 or electronic information, there is reasonable necessity for the seizure for the reasons set
 4 forth above. *See* 18 U.S.C. § 3103a(b)(2).

5 49. I further request that the Court direct T-Mobile to disclose to the
 6 government any information described in Attachment B2 that is within the possession,
 7 custody, or control of T-Mobile. I also request that the Court direct T-Mobile to furnish
 8 the government all information, facilities, and technical assistance necessary to
 9 accomplish the collection of the information described in Attachment B2 unobtrusively
 10 and with a minimum of interference with T-Mobile's services, including by initiating a
 11 signal to determine the location of the Target Telephone on T-Mobile's network or with
 12 such other reference points as may be reasonably available, and at such intervals and
 13 times directed by the government. The agency shall reasonably compensate T-Mobile for
 14 reasonable expenses incurred in furnishing such facilities or assistance.

15 50. Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant
 16 by serving the warrant on T-Mobile. Because the warrant will be served on T-Mobile,
 17 who will then compile the requested records and data, reasonable cause exists to permit
 18 the execution of the requested warrant at any time in the day or night. I therefore request
 19 that the Court authorize execution of the warrant at any time of day or night, owing to the
 20 potential need to locate the Target Cell Phone outside of daytime hours.

21 **AUTHORIZATION REQUEST FOR TARGET VEHICLE 2**

22 51. As set forth above, based on the facts set forth in this affidavit, there is
 23 probable cause to conclude that violations of 21 U.S.C. § 841 and § 846 (distribution of
 24 controlled substances and conspiracy to distribute controlled substances) have been
 25 committed, are being committed, and will be committed by the user of **TT2** and the
 26 driver of **TV2**, and others. Tracking the location of **TV2** will help law enforcement
 27 monitor its users, follow their movements when they are at locations that are otherwise
 28 hard for law enforcement to observe, and identify other coconspirators, sources of supply,

1 storage locations, and other people and places of evidentiary value. There is probable
2 cause to believe that the use of the investigative technique described by the warrant will
3 result in officers learning that identifying information.

4 52. As discussed above, I am requesting permission to install/service the
5 tracker(s) at any time, day or night, in order to ensure that we can do so covertly and
6 avoid jeopardizing the ongoing investigation. Because we believe early morning hours or
7 later evening hours are the safest time for installation and access to the vehicle, we
8 request nighttime authorization. Additionally, we request to be authorized to access the
9 following addresses to install or maintenance the tracking device:

- 10 a. 2728 175th Street SE Bothell, Washington, 98012 (owner's address)
11 b. 7443 NE 146th Street Kenmore, Washington, 98028 (where **TV2**
was located after the controlled purchase).

12 53. I seek authority to do the following: (a) install, remove, monitor, repair, or
13 adjust a global positioning satellite (hereinafter GPS) electronic tracking device on to
14 **TV2** at any time of the day or night; (b) if necessary to protect the safety of person
15 installing, removing monitoring, repairing, or adjusting the electronic tracking device on
16 **TV2**, or to protect the integrity of the investigation, to surreptitiously enter the subject
17 vehicle at any time of the day or night, and move the subject vehicle from one location to
18 another for the purpose of installing, removing, monitoring, repairing, or adjusting the
19 device; and/or to tow the vehicle; (c) surreptitiously re-enter **TV2** at any time of the day
20 or night, for the purpose of installing, removing, monitoring, repairing, or adjusting the
21 device; and (d) continuously monitor any and all signals emitted from the electronic
22 tracking device in any jurisdiction within the United States, including when the vehicle
23 enters any structure or private property in which there may be a reasonable expectation of
24 privacy. I request this authorization for a period of up to forty-five (45) days.

25 54. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of
26 Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to
27 delay notice to the owner(s) or user(s) of the Target Vehicle until 90 days after the
28

1 collection authorized by the warrant has been completed. There is reasonable cause to
 2 believe that providing immediate notification of the warrant may have an adverse result,
 3 as defined in 18 U.S.C. § 2705. Providing immediate notice to the user(s)/owner(s) of
 4 the Target Vehicle would seriously jeopardize the ongoing investigation, as such a
 5 disclosure would give that person an opportunity to destroy evidence, change patterns of
 6 behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1).

7 55. I further request that the Court order that all papers in support of this
 8 application, including the Affidavit and Tracking Warrant, be sealed until further order of
 9 the Court. These documents discuss an ongoing criminal investigation that is neither
 10 public nor known to all of the targets of the investigation. Accordingly, there is good
 11 cause to seal these documents because their premature disclosure may seriously
 12 jeopardize that investigation.

13 **FACEBOOK SOCIAL NETWORKING SERVICES**

14 56. Facebook owns and operates a free-access social networking website of the
 15 same name that can be accessed at <http://www.facebook.com>. Facebook allows its users
 16 to establish accounts with Facebook, and users can then use their accounts to share
 17 written news, photographs, videos, and other information with other Facebook users, and
 18 sometimes with the general public.

19 57. Facebook asks users to provide basic contact and personal identifying
 20 information to Facebook, either during the registration process or thereafter. This
 21 information may include the user's full name, birth date, gender, contact e-mail
 22 addresses, Facebook passwords, Facebook security questions and answers (for password
 23 retrieval), physical address (including city, state, and zip code), telephone numbers,
 24 screen names, websites, and other personal identifiers. Facebook also assigns a user
 25 identification number to each account.

26 58. Facebook users may join one or more groups or networks to connect and
 27 interact with other users who are members of the same group or network. Facebook
 28 assigns a group identification number to each group. A Facebook user can also connect

1 directly with individual Facebook users by sending each user a “Friend Request.” If the
2 recipient of a “Friend Request” accepts the request, then the two users will become
3 “Friends” for purposes of Facebook and can exchange communications or view
4 information about each other. Each Facebook user’s account includes a list of that user’s
5 “Friends” and a “News Feed,” which highlights information about the user’s “Friends,”
6 such as profile changes, upcoming events, and birthdays.

7 59. Facebook users can select different levels of privacy for the
8 communications and information associated with their Facebook accounts. By adjusting
9 these privacy settings, a Facebook user can make information available only to himself or
10 herself, to particular Facebook users, or to anyone with access to the Internet, including
11 people who are not Facebook users. A Facebook user can also create “lists” of Facebook
12 friends to facilitate the application of these privacy settings. Facebook accounts also
13 include other account settings that users can adjust to control, for example, the types of
14 notifications they receive from Facebook.

15 60. Facebook users can create profiles that include photographs, lists of
16 personal interests, and other information. Facebook users can also post “status” updates
17 about their whereabouts and actions, as well as links to videos, photographs, articles, and
18 other items available elsewhere on the Internet. Facebook users can also post information
19 about upcoming “events,” such as social occasions, by listing the event’s time, location,
20 host, and guest list. In addition, Facebook users can “check in” to particular locations or
21 add their geographic locations to their Facebook posts, thereby revealing their geographic
22 locations at particular dates and times. A particular user’s profile page also includes a
23 “Wall,” which is a space where the user and his or her “Friends” can post messages,
24 attachments, photographs and links that will typically be visible to anyone who can view
25 the user’s profile (subject to the privacy settings selected by the account user).

26 61. Facebook has a Photos application, where users can upload an unlimited
27 number of albums and photos. Another feature of the Photos application is the ability to
28 “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a

1 photo or video, he or she receives a notification of the tag and a link to see the photo or
2 video. For Facebook's purposes, the photos associated with a user's account will include
3 all photos uploaded by that user that have not been deleted, as well as all photos uploaded
4 by any user that have that user tagged in them.

5 62. Facebook users can exchange private messages on Facebook with other
6 users. These messages, which are similar to e-mail messages, are sent to the recipient's
7 "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well
8 as other information. Facebook users can also post comments on the Facebook profiles
9 of other users or on their own profiles; such comments are typically associated with a
10 specific posting or item on the profile. In addition, Facebook has a Chat feature that
11 allows users to send and receive instant messages through Facebook. These chat
12 communications are stored in the chat history for the account. Facebook also has a Video
13 Calling feature, and although Facebook does not record the calls themselves, it does keep
14 records of the date of each call.

15 63. If a Facebook user does not want to interact with another user on Facebook,
16 the first user can "block" the second user from seeing his or her account.

17 64. Facebook has a "like" feature that allows users to give positive feedback or
18 connect to particular pages. Facebook users can "like" Facebook posts or updates, as
19 well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook
20 users can also become "fans" of particular Facebook pages.

21 65. Facebook has a search function that enables its users to search Facebook for
22 keywords, usernames, or pages, among other things.

23 66. Each Facebook account has an activity log, which is a list of the user's
24 posts and other Facebook activities from the inception of the account to the present. The
25 activity log includes stories and photos that the user has been tagged in, as well as
26 connections made through the account, such as "liking" a Facebook page or adding
27 someone as a friend. The activity log is visible to the user but cannot be viewed by
28 people who visit the user's Facebook page.

1 67. Facebook Notes is a blogging feature available to Facebook users, and it
2 enables users to write and post notes or personal web logs (“blogs”), or to import their
3 blogs from other services, such as Xanga, LiveJournal, and Blogger.

4 68. The Facebook Gifts feature allows users to send virtual “gifts” to their
5 friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase,
6 and a personalized message can be attached to each gift. Facebook users can also send
7 each other “pokes,” which are free and simply result in a notification to the recipient that
8 he or she has been “poked” by the sender.

9 69. Facebook also has a Marketplace feature, which allows users to post free
10 classified ads. Users can post items for sale, housing, jobs, and other items on the
11 Marketplace.

12 70. In addition to the applications described above, Facebook also provides its
13 users with access to thousands of other applications on the Facebook platform. When a
14 Facebook user accesses or uses one of these applications, an update about that the user’s
15 access or use of that application may appear on the user’s profile page.

16 71. Facebook uses the term “Neoprint” to describe an expanded view of a given
17 user profile. The “Neoprint” for a given user can include the following information from
18 the user’s profile: profile contact information; News Feed information; status updates;
19 links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists,
20 including the friends’ Facebook user identification numbers; groups and networks of
21 which the user is a member, including the groups’ Facebook group identification
22 numbers; future and past event postings; rejected “Friend” requests; comments; gifts;
23 pokes; tags; and information about the user’s access and use of Facebook applications.

24 72. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP
25 address. These logs may contain information about the actions taken by the user ID or IP
26 address on Facebook, including information about the type of action, the date and time of
27 the action, and the user ID and IP address associated with the action. For example, if a
28

1 user views a Facebook profile, that user's IP log would reflect the fact that the user
2 viewed the profile, and would show when and from what IP address the user did so.

3 73. Social networking providers like Facebook typically retain additional
4 information about their users' accounts, such as information about the length of service
5 (including start date), the types of service utilized, and the means and source of any
6 payments associated with the service (including any credit card or bank account number).
7 In some cases, Facebook users may communicate directly with Facebook about issues
8 relating to their accounts, such as technical problems, billing inquiries, or complaints
9 from other users. Social networking providers like Facebook typically retain records
10 about such communications, including records of contacts between the user and the
11 provider's support services, as well as records of any actions taken by the provider or
12 user as a result of the communications.

13 74. Therefore, the computers of Facebook are likely to contain all the material
14 described above, including stored electronic communications and information concerning
15 subscribers and their use of Facebook, such as account access information, transaction
16 information, and other account information.

17 75. On October 12, 2021, a preservation letter was sent to Facebook, which
18 asked Facebook to preserve the contents of the account identified above, under authority
19 of Title 18, United States Code, Section 2703(f)(1), for a period of 90 days.


20 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

21 76. I anticipate executing this warrant under the Electronic Communications
22 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by
23 using the warrant to require Facebook to disclose to the government copies of the records
24 and other information (including the content of communications) particularly described in
25 Section I of Attachment B3. Upon receipt of the information described in Section I of
26 Attachment B3, government-authorized persons will review that information to locate the
27 items described in Section II of Attachment B3.
28

REQUEST FOR NONDISCLOSURE AND SEALING

77. I request, pursuant to the preclusion-of-notice provisions of Title 18, United States Code, Section 2705(b), that Facebook be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The government submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, and to continue his flight from prosecution.

78. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing fugitive investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation by making the targets aware of the pending investigation and allowing them an opportunity to destroy evidence related to this investigation.


 Joseph Kirby, Affiant
 TFA
 Drug Enforcement Administration

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 22nd day of October, 2021.



 PAULA McCANDLIS
 United States Magistrate Judge

EXHIBIT 1

DECLARATION

I, Stephen Hobbs, declare as follows:

1. I am a duly appointed Assistant United States Attorney for the Western District of Washington, and I have primary responsibility for representing the interests of the United States herein.

2. I make this declaration in support of an application for a search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) with an integrated pen-trap order pursuant to 18 U.S.C. §§ 3122 and 3123. Pursuant to 18 U.S.C. § 3122(a)(1), I am the applicant for purposes of the pen-trap portion of the requested warrant and order.

3. Pursuant to 18 U.S.C. § 3122(b), I certify that the DEA is the law enforcement agency conducting the investigation in this matter and that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by that agency.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing Application is made on the basis of information officially furnished, and on that basis I verily believe such information to be true.

Executed this 22nd day of October 2020.

/s/ Stephen Hobbs

Stephen Hobbs

Assistant United States Attorney

ATTACHMENT A2**Property to Be Searched and Subscriber/Subject Information**

1. Records and information associated with the cellular phone assigned call number (360) 230-0625, ("Target Telephone 2" or the "Target Phone"), that are in the custody or control of T-Mobile, a company headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054. The subscriber/customer of the Target Cell Phone is "Mario GARCIA" with an address of "11400 NE 132nd Street Apt B106 Kirkland, Washington, 98034-4752,". The identity of the person who is the subject of the criminal investigation is unknown.

2. The property to be searched includes: (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number assigned to an instrument now bearing the same unique identifying number (such as an IMSI, ESN, MSID, or IMEI) as the telephone number listed above, or that was bearing the same unique identifying number as the telephone number listed above, at any point within the last 30 days, (iii) any changed unique identifying number subsequently assigned to the same telephone number, or (iv) any additional changed telephone number and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone numbers listed above, within the period of disclosure authorized by this warrant.

In Attachment B2, T-Mobile may be referred to as the "Wireless Provider."

ATTACHMENT B2

Particular Things to be Seized

This warrant is issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2713, and the Pen Register Act, 18 U.S.C. §§ 3121-3127. As such, this warrant authorizes the collection of subscriber records, pen-trap data, and cell site data information regarding the Target Cell Phone. **This warrant does not authorize the disclosure or seizure of any tangible property or the content of any wire or electronic communication, as defined in 18 U.S.C. § 2510(8).** Accordingly, the Court finds reasonable necessity for the seizure of the data and records identified below. *See* 18 U.S.C. § 3103a(b)(2).

I. Section I: Information to be Disclosed by T-Mobile

1. **Subscriber/Account Information.** The following non-content information about the customers or subscribers associated with the Account listed in Attachment A2:

- a. Names (including subscriber names, user names, and screen names);
- b. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- c. Local and long distance telephone connection records from September 21 to October 22, 2021;
- d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions from September 21, 2021 to October 22, 2021;
- e. Length of service (including start date) and types of service utilized;
- f. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital